Claim 55, line 2, Change "such" to --said--;

Change "request" to --requests--.

Claim 56, line 2, Change "such" to --said--;

Change "request" to --requests--.

Claim 59, line 2, Change "includes" to --include--.

Claim 60, line 2, Change "includes the" to --include a--.

Claim 64, line 2, Change "the" to --a--.

Claim 78, line 1, Change "the", second occurrence, to --a--.

Claim 79, line 1, Change "the", second occurrence, to --a--;

Line 2, Change "the" to --a--.

REMARKS

The claims have been checked, and the changes set forth above are to improve the clarity and accuracy with which the inventions are claimed. Claim 5 has been re-written to clarify changes previously intended to have been made in the preliminary amendment.

Reconsideration is respectfully requested for claims 1-81 (as amended) which have been rejected on various grounds as follows:

Claims 1-81 have been rejected as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, the

Office Action alleging that "The claims are indefinite because Internet and Intranet are two different concepts, therefore the scope of the claims cannot be determined (in claim 1, element b, and claim 42 element c)." In response to this observation, Applicant would respectfully show that the offending expression "internet and/or intranet" has been deleted and that the claims now recite "means including interconnected computers" (Claim 1) and "through an interconnected computer input terminal" (Claim 42). Accordingly, and in view of the foregoing, it is respectfully requested that this ground of rejection be withdrawn.

Claims 1-81 have also been rejected under 35 USC 103(a) as being unpatentable over Evans U.S. Patent 5,924,074, the Office Action stating:

" . . . . Evans does not specifically disclose a data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data and, when said request fails to comply with said conditions, for denying access to said data. However, Evans does disclose a method and system comprising the steps of organizing the patient data so as to form a patient record, and retrieving the patient record to access the patient data for use in the care of a patient, and obtaining a patient identifier, locating a patient record corresponding to the patient identifier

(which is readable as data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data)" (citing column 3, lines 10-35).

The Action continues "It would have been obvious to a person of ordinary skill in the art at the time the invention was made to have modified the teachings of Evans with data processing means responsive to a request for patient medical data for comparing said request with said conditions required for access of said data, thereby improving the accuracy and reliability of standing order database search system and method for Internet and Intranet application"

In response to this conclusion, Applicant avers that such conclusion by the Examiner is unsupported by any implicit or explicit suggestion of, or any motivation for, the desirability of such modification, in the Evans patent itself or elsewhere. As such, the conclusion of "obviousness" made by the Examiner is nothing but unsupported opinion, and not a proper basis for rejection. In this connection, it is Applicant's understanding that the Examiner is required to identify where the prior art provides a motivating suggestion for the modification as for example in the decision in *In re Jones,* 21 USPQ 2d 1941 (Federal Circuit, 1992) where the court held: "Before the PTO may combine the disclosures of two or more prior art references in order to

establish *prima facie* obviousness, there must be some suggestion for doing so . . . *In re Fine*, 5 USPQ 2d 1596, 1598-99 (Fed Cir 1988)" [at 1943] (Emphasis Added). "The prior art must provide one of ordinary skill in the art the motivation to make the proposed molecular modifications needed to arrive at the claimed compound." [at 1944] (Emphasis added).

Moreover, the courts have advocated that even if the prior art may be modified as suggested by the Examiner, the modification is not obvious unless the prior art suggests the desirability for the modification as, for example, in the decision in *In re Fritch* 23 USPQ 2d 1780 (Fed Cir 1992), where the court held: "Mere fact that prior art may be modified to reflect features of claimed invention does not make modification, and hence claimed invention obvious unless desirability of such modification is suggested by prior art . . ." [at 1780] (Emphasis Added).

It has also been held that the motivation suggestion must be explicit, as was decided in the case of *Winner International Royalty Corp. v. Wang*, 48 USPQ 2d 1139 (D.C.D.C. 1998), where the court held: " . . .invention cannot be found obvious unless there was some explicit teaching or suggestion in art to motivate one of ordinary skill to combine elements so as to create same invention." [at 1140] (Emphasis Added). . . . "there must have been some explicit teaching or suggestion in the art to motivate

one of ordinary skill to combine such elements so as to create the same invention" [at 1144] (Emphasis Added).

In further response to the foregoing, Applicant would respectfully show that, despite diligent search, he has been unable to find any teaching or suggestion (**implicit or explicit**) in either the Evans reference or any other art of which he is aware, of the automatic denial of access to a patient's record until a comparison of a request for a patient's record meets criteria required for access thereto. Moreover, in support of an assertion of unobviousness, Applicant would respectfully show that Applicant's claimed invention meets an important need long felt in the art, a compelling argument in support of patentability. As examples of such long and generally recognized need, Applicant presents the documents set forth in Annexes A, B and C to this Amendment. These documents are:

Annex A *A Summary of References Which Demonstrate Both the Novelty and Demand for Allcare's Privacy Service*

Annex B *Online Healthcare Gets Candid Assessment at Berkeley Summit*

Annex C *Privacy Technology Still Missing the Mark*

In reviewing the foregoing Annexes, it is dramatically evident that some of the most inquiring and influential minds have given much attention and thought to the importance of maintaining patient privacy while providing for legitimate

controlled access to their medical records yet without having achieved the *inspirational insight* manifest in Applicant's claimed subjects. While, in hindsight, such may seem more modest, it is well settled that although a "difference may have seemed slight (as has often been the case with some of history's great inventions, e.g., the telephone), [but] it may also have been the key to success and advancement in the art resulting from the invention." (*Jones et al v Hardy*, 220 USPQ 1021 CAFC 1984)(Underscoring Added). Applicant asserts that such is the case with the instant application.

In further support of unobviousness and consequent patentability of the instant claims, it has been observed authoritatively that "It is usually the application of old principles to new methods or articles of manufacture that involved patentable subject matter." (*In re Watter* 64 USPQ 571 CCPA 1945, at page 573) Moreover, as Judge Learned Hand observed, "It is the obvious when discovered and put to use that most often proves invention." (*H. C. White Co v Morton E. Converse & Son Co.*, 2 Cir., 20 F. 2d 311, 313)

As the Examiner is undoubtedly aware "Evidence of secondary considerations may often be the most probative and cogent evidence in the record. It may often establish that an invention appearing to have been obvious in light of the prior art was not." (*Stratoflex Inc v Aeroquip Corp*, 218 USPQ 879, CAFC 1983)

(Underscoring added). Since it is well known that satisfaction of a well known and long felt need is an important secondary consideration, Applicant believes it evident that the subjects defined by the independent Claims 1 and 42 are unobvious and patentable not only over the Evans reference but all other art of which Applicant is aware. Accordingly, it is respectfully requested that the rejection of Claims 1 and 42 be withdrawn.

The remaining claims, i.e., Claims 2-41 and 43-81, are seen to be dependent to Claims 1 and 42 and include additional features and limitations thereover. Accordingly, it is believed that for the reasons set forth with respect to Claims 1 and 42, they also are unobvious and patentably distinct from the prior art; and their allowance is respectfully solicited.

Applicant has reviewed the remaining patents cited but not applied against the claims but finds nothing in any of them which teaches or suggests the subject matter of the claims.

SUMMARY

Summarizing, the claims have been carefully checked and changes made to improve the clarity and accuracy with which the inventions are claimed. Claims 1 and 42 have been amended to eliminate any indefiniteness and thereby overcome the rejection under 35 USC 112. The claims also have been shown to recite subject matter that is unobvious over the Evans reference; and

Applicant is unaware of any other art which either singly or in combination teaches or suggests the subject matter defined by the claims. Accordingly, it is requested that the claims be allowed and that the case be advanced to issue.

Respectfully,

Andrew M. Hassell
Registration No. 18182
Attorney for Applicant
12568 Burninglog Lane
Dallas, Texas 75243
Tel: (972) 234-6540
Fax: (972) 234-6540

CERTIFICATE OF MAILING

I hereby certify that the above-noted paper is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D. C. 20231, on September 5, 2000.

Andrew M. Hassell

annex a

PRIVACY APPLICATION

A SUMMARY OF REFERENCES WHICH DEMONSTRATE BOTH THE NOVELTY AND DEMAND FOR ALLCARE'S PRIVACY SERVICE

Allcare™ Health Management System, Inc. has filed a patent application on a database search facility that contains a number of unique elements, including the ability to efficiently share patient records among authorized persons and simultaneously allow for informed consent to assure that individual pricacy considerations are addressed.

The following quotes and referenced documents, which were gathered contemporanously with the filing of the patent application evidence the novelty of the approach as well as the propsective widespread demand for the service.

The San Jose Mercury News, a widely recognized online resource for Silicon Valley companies reported the following headline in its March 4, 1997 Morning edition: "The electronic privacy issue is shaping up as a major-league battle in the 105th Congress, where more than a dozen new bills have been introduced this session. On the eve of the annual *Computers, Freedom & Privacy conference* March 11-14 in Burlingame, *Salon magazine* talks with Marc Rotenberg, co-founder of the *Electronic Privacy Information Center*, about the political climate enveloping the issue."

Wired Magazine covered the issue from a different angle in a March 5, 1997 story entitled *Panel Urges Medical Data Protection*, which noted: "Right now, if your medical records are on a computerized database or are transmitted, you run the risk of having them seen by people you never dreamed would be perusing your health information." The story also references a National Research Foundation *advisory panel report* funded by the National Library of Medicine, the Warren Grant Magnuson Clinical Center of the National Institutes of Health, and the Massachusetts Health Data Consortium which urges "industry standards, regulatory action, and pressure from consumers . . . to bolster the privacy and security of electronic patient records."

These resources, together with the written and oral testimony before various Congressional committees and other sources describe the state of the technology and law at the time Mr. Shelton's system and method patent application was filed. The following sections present highlights from the subcommittee hearings with regard to *H.R. 52. Fair Health Information Practices Act of 1997*, a bill introduced by *Rep. Condit* (D-CA) on January 7, 1997, to establish a code of fair information practices for health information, to amend section 552a of title 5, United States Code, and for other purposes.

FROM TESTIMONY BEFORETHE NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, SUBCOMMITTEE ON PRIVACY AND CONFIDENTIALITY
(January 13-14, 1997)

In his opening remarks, Dr. Robert Gellman, a privacy and information policy consultant in Washington and the subcommittee chair stated: "We intend to cover the full range of fair information practices issues, including patient's rights, limits on use and disclosure of information, health identification numbers, pre-emption of state laws and privacy-enhancing technologies when available, sometimes known as PETs -- privacy-enhancing technologies."

The subcommittee's first witness was Dr. David Korn, Professor of Pathology, and immediate past Vice President of Stanford University, Dean of the Stanford Medical School and a distinguished scholar in residence at the AAMC. *Dr. Korn's testimony* provides an excellent summary of the witnesses who testified during the two days. He stated: "The difficult challenge before this committee is to find a point of balance that will enable to us to enhance the security of confidential medical information and reduce the probability of its misuse, without substantially impairing the access and communication that are essential to the effective delivery of medical care, the efficient functioning of the health care delivery system and the pace of biomedical and health services research.

"But given the requirements for access and communication in the real worlds of medical care and biomedical research, *such levels of security in my judgment are fanciful*. More realistic would be to develop the best security mechanisms feasible from a cost benefit perspective, and couple that effort with effective measures to prohibit the discriminatory misuse of such information by employers, insurance companies or others.

"Unfortunately, we as a society have not succeeded in reaching that objective. In the absence of such effective measures, much effort is directed toward restricting the creation and accessibility of information, and building firewalls to insure its confidentiality."

Dr. Elizabeth Andrews, Chairperson for the Committee on Data Privacy of the International Society for Pharmacoepidemiology (ISPE), the director of epidemiology for Glaxo Wellcome and an adjunct associate professor of epidemiology at the University of North Carolina School of Public Health, stated: "Our studies often require data from files years after the medical events in question, years after patients have left a particular health plan, and sometimes after patients have died. *Requiring authorization for each research use is simply not feasible*."

FROM TESTIMONY BEFORETHE NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, SUBCOMMITTEE ON PRIVACY AND CONFIDENTIALITY
(February 3-4, 1997)

On February 3, 1997, David L. Larsen, Director of Health Care Services at Salt Lake City-based Intermountain Health Care (IHC), testifyied on behalf of the American

Association of Health Plans (AAHP) which represents 1,000 HMOs, PPOs, and similar network plans providing care to over 120 million Americans. *In his testimony, Mr. Larsen stated*: "AAHP supports this Committee's efforts to protect against the unauthorized and inappropriate use of patient information while at the same time facilitate the coordination and delivery of high quality, network-based health care. It is important that your recommendations recognize the special needs of integrated delivery systems.

"In order to manage and improve the health outcomes of the population we insure, we must be able to share information among IHC corporate entities -- our physicians, hospitals, and health plans. IHC has developed electronic medical records and common databases to facilitate this communication. Preventing the creation of these common databases, limiting the type of data which can be shared within the IHC integrated delivery system, or *requiring a patient's authorization for each and every transaction and transfer of data*, would severely limit IHC's ability to measure and improve the health outcomes of our enrollees."

Also on February 3, Jeanne Scott, Director of Government and Legal Affairs for Oklahoma-based CIS Technologies, Inc., a subsidiary of National Data Corporation (NDC), testified on behalf of the Association for Electronic Health Care Transactions (AFEHCT), a trade organization who's member companies process over 2 billion electronic transactions annually. *In her testimony, Ms. Scott said*: "CIS and NDC support workable systems that will OPTIMIZE individual protections and assure that the advantages offered by the EDI and electronic commerce in health care will not be outweighed by the costs to individual privacy and personal freedom."

She later clarified: "But OPTIMIZATION does not mean maximization . . . . We cannot allow such an important issue [as reducing the cost of healthcare through greater use of computer-based patient records systems] to get bogged down in a shouting contest among the players and participants. Each must try to recognize and work together in seeking OPTIMIZATION all sides have to be open to the needs of our society and our technological capabilities in addressing these needs effectively and cost-efficiently."

Robert B. Burleigh, President of Brandywine Healthcare Services and Consultant to the Board of Directors of the International Billing Association (IBA), the only trade association representing third party medical billing companies, also testified before the National Committee on Vital and Health Statistics Subcommittee on Privacy and Confidentialityon February 3, 1997. *In his testimony, Mr. Burleigh addressed* various provisions of H.R. 51, proposed legislation to create nationally uniform standards for the confidentiality of health information to assure the safety of the shared information.

In his remarks with respect to Subtitle B - Use and Disclosure of Protected Health Information - Section 111(d), Mr. Burleigh stated: "This section provides that a 'health information trustee may disclose protected health information only if the recipient has been notified that the information is protected health information....' In the normal course of business today, *the technical means of notifying a recipient of (proposed) protected health information, prior to, or concurrently with, disclosure does not exist*. In practice, it would be necessary to identify, with specificity, the information subject

to protection, since some information may be protected in some, but not all instances." Accordingly, he recommended that the "section should be revised to conform with the reality of the flow of medical records information."

In his remarks with regard to Section 112. Authorizations for Disclosure of Protected Health Information, Mr. Burleigh added: "We are concerned that the legislation proposes eight separate elements before a disclosure can be made. In the ordinary course of business, many forms are used to accomplish the same function for multiple providers, particularly in a hospital-based setting. In addition, identification of the payer(s) to receive the information, and the information they will require (the subject of the consent) at the time of consent (crucial to informed consent) is often not possible. The remedy would be both inconvenient and intrusive to the patient and the provider(s)."

And he concluded with the following warning: "We are concerned that an unintended result of this proposed legislation would be the decision by providers to discontinue accepting insurance coverage in order to avoid the burdensome (in their view) new duties of securing informed consents, providing disclosures, maintaining new disclosure logs and related records, and other proposed responsibilities."

On February 4, 1997, Robert Thompson, Vice President of Pharmacy Operations for Revco Drug Stores, testified as a representative of his organization, which operates 2,500 pharmacies in 17 states, and an example of the community pharmacy infrastructure which extends beyond 54,000 retail pharmacies, providing over 60% of the 2.4 billion out-patient prescriptions dispensed annually.

During his testimony, Mr. Thompson states that although his organization "fully supports the intent of federal standards to preserve the confidentiality of patient-identifiable health care information . . . [w]e urge you to consider the real-time impact of requiring patient authorization for the disclosure of patient identifiable information."

Whereas the Total Access design will permit each record repository to set its own standards in accordance with local law, Mr. Thompson shows that this flexibility is not present, nor contemplated, in any of the system designs he is aware of when he stated: "Without total preemption [of state confidentiality laws by federal law], *we will find it impossible to integrate the necessary patient information and authorizations in our computer software. Electronic transmission will become ineffective*."

He concludes by saying: "We believe that the effective date of any legislation should reflect the uncertainty of the unknown costs and technology needed to implement a new federal law. Adequate time must be allowed for software manufacturers to develop their products, to test and distribute the product, and to train [personnel to use them]." Whereas the estimated time to write the Allcare Total Access system is less than 6 months, he asks for 24 months to accomplish this.

FROM TESTIMONY BEFORETHE NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, SUBCOMMITTEE ON PRIVACY AND CONFIDENTIALITY
(February 18-19, 1997)

On February 18, Lauren Dame, staff attorney at Public Citizen's Health Research Group, a non-profit organization founded in 1971 by Ralph Nader and Dr. Sidney Wolfe, testified before the committee. *In her prepared remarks, Ms. Dame stated:* "As medical records are computerized and there is increased disclosure of sensitive medical information -- as we believe there will be -- many of the problems consumers face today will be exacerbated unless strong privacy protections are included in any regulations developed. . . . [P]rivacy for medical information is an important value in and of itself. People feel very strongly that they should have control over the dissemination of what amounts to highly intimate and private information about themselves.

"[W]e believe that any effort to regulate the use and development of computerized patient medical records should begin with the proposition that . . . personally identifiable patient information should not be disclosed without the informed consent of the patient. (And, by "informed consent", I do not mean the kinds of blanket consent or release forms patients currently are forced to sign in order to obtain health insurance, which basically give the insurers the right to collect any medical information they want, and to do with it what they will.)"

Ms. Dame concluded her remarks with this statement which indicates the solutions have yet to be devised: "[Y]ou have heard from insurers, providers, and processors of data, and no doubt most of them have painted glowing pictures of the great increases in efficiency and cost savings associated with computerizing medical records and with limiting privacy protections. While in some areas, the interests of all of us might be accommodated, often you will be faced with some hard choices.

"In making your recommendations to the Secretary, I urge you to err on the side of protecting the privacy and confidentiality of personally-identifiable medical information. As a society, we can always modify regulations to increase data exchange *if experience shows us that we can safely do so*. But privacy, once lost, cannot be recaptured."

On February 19, 1997, Dr. Denise Nagel, a physician, instructor at Harvard Medical School and co-founder of the National Coalition for Patient Rights, an organization whose mission is to protect and preserve privacy and confidentiality in medical care, testifyied for that organization and on behalf of the American Psychoanalytic Association and the Association of American Physicians and Surgeons. *During her testimony, Dr. Nagel quoted* the 1996 Time/CNN poll which "found that 87% of Americans believed that 'laws should be passed that prohibit health care organizations from giving out medical information without first obtaining the patient's permission.'" and commented that "the same percentage of people in a 1993 Louis Harris poll trusted their own providers but most (71%) believed that 'if privacy is to be preserved, the use of computers must be sharply restricted in the future.'" Dr. Nagel stated her opinon: "Rules that conform to these views would require consent for placing personal information in a computer system and consent for the disclosure of identified information, except in rare circumstances."

She concluded her remarks with the following statement: "The organizations that I

represent do not have all the answers, but we have a principled approach grounded in the legal, ethical and medical history of our country." It is reasonable to assume that were Dr. Nagel aware of the functionality within the Total Access system, she would have had a solution to offer that would be consistent with her principle-based concerns.

Such an approach would fulfill her concluding comments, made in response to a question from the Committeee chairperson: "The need to protect, preserve *and in some instances restore, the right to medical privacy* in order to preserve quality medical care could hardly be more widely recognized. This Committee has the opportunity to enhance the quality of health care by recommending privacy standards which are consistent with the right to privacy recognized under the Constitution, statutory law, and hundreds of years of medical ethics. Alternatively, this Committee can perpetuate *the current chaotic conditions that are eroding the essential bond of trust between the patient and the treating physician*. We ask the Committee to advance the cause of quality health care, not retard it.

On February 14, 1997, Patrick E. McFarland, the Inspector General of the Office of Personnel Management, the federal agency that oversees the Federal Employees Health Benefits Program (FEHBP), the third-largest health care expenditure program for the United States, testified before the subcommittee. This letter was entered into the record following the subcommittee's February 19, 1997 session. *In his written statement, Mr. McFarland testified*: "Although it is usually not necessary to examine patient treatment records, the additional information obtained through these law enforcement tools are an integral part of anal ing and building a successful case. We must use patient records to determine whethe there is a fraudulent pattern of billing or use of patients in schemes to obtain benefits f unnecessary services. My office recognizes the concerns of the public with res ect to confidentiality of medical records and mandates a policy to limit our requests to only information necessary for the investigation. *We consider all legal safeguar before disclosing any medical information* to other federal agencies or other individuals.

"With these procedures in place, *any increased restrictions such as a probable cause and notice requirement* for subpoenas contained in recent legislative proposals including HR. 52, The Fair Health Information Practices Act of 1997, *would create what I believe to be an unnecessary and insurmountable burden* on this Office of Inspector General. With a limited staff, adding additional hurdles beyond the present standard of relevancy to the process for accessing medical information would increase the likelihood of litigation at an early investigative stage and would therefore considerably limit the ability to effectively and efficiently investigate, prosecute and deter health care fraud."

Andrew B

Andrew Hassell

From: "Robert H. Shelton" <RbtShelton@worldnet.att.net>
To: "Andrew M Hassell" <ahassell@prodigy.net>
Cc: "Halden Conner" <hconner1@aol.com>; "John Sigalos" <jlsig1@airmail.net>
Sent: Thursday, June 29, 2000 4:44 PM
Subject: Berkeley Summit Points to Privacy as Critical Issue

See attached article expressing challenges with privacy of individual medical records, and how important a solution to the issue is to the whole industry's future.

I continue to feel that our pending "Private Access" patent application addresses this impediment extremely well. I'm wondering whether we should be providing this kind of article to the USPTO to emphasize that the problem we described in the application is still very much present.

Also, it sure seems like a long time has transpired since we filed that application, with no reply. Should we be checking on its status, if for no other reason than just to make certain nothings been lost in transit...?

<< ONLINE HEALTHCARE GETS CANDID ASSESSMENT AT BERKELEY SUMMIT

Online healthcare has a long, but promising, road ahead of it, according to some scientists and venture capitalists assessing the state of e-health. At the International Biotech and Infotech Summit in Berkeley this week, attendees said that while the Internet is currently changing science, there is still concern that profitable business models are rare in the world of e-health. Summit participants concluded that Web-based medical records, insurance claims, and prescriptions will eventually succeed, but existing technology can't currently handle the data. Additionally, privacy standards and uniform applications need to be in place before both physicians and patients feel confident in e-healthcare.

View full text: http://www.epharm5.com/news.asp?an=APRS0017939018 >>

<< Online health care, which right now is largely limited to informational and pharmacy Web sites such as PlanetRx.com and WebMD.com, has been hyped a great deal. But profitable business models - and reasons for investing - are few and far between, Colella said.

To be sure, the Internet could streamline medical records, insurance claims and prescriptions, but the computing power needed to handle all that data is several years away, panelists said. And until better technology and viable business models come along, investing in e-health care is "still an incredibly high risk," Colella said.

Thus far the only profits associated with online health care have come from business-to-business transactions such as medical supply auctions, and from shepherding online "communities" of patients toward products that interest them, panelists said.

But the roadblocks to the one-click health care system of the future are not just about business models and technology. Medical records are another frontier.

Putting records online would make it possible for any doctor anywhere to see a patient's comprehensive medical history, thus avoiding duplicate tests and making it far easier to diagnose illness.

But Americans are still not comfortable enough with security on the Web to put their records online, said Dr. Mark McClellan, an assistant professor at Stanford University's Center for Health Policy.

"There's still a fundamental perception problem of whether people think medical records online are safe," McClellan said. "Most Americans do not think so."

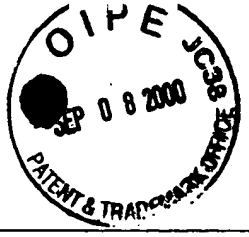
Providing such widespread access to medical histories also raises ethical questions, McClellan said....

The fear is that if medical records or genetic information about individual humans gets into the wrong hands - particularly if it happens long before cures are developed - discrimination could result.

Complicating matters further, there is no standard medical-record format that every hospital, insurance provider and doctor uses, McClellan said. All these health care entities would have to agree on a format before the information could be put online with any efficiency, he said.

Despite the obstacles, the experts at Tuesday's conference, entitled "Into the 21st Century: Genomics and Beyond," were still enthusiastic about online health care's potential.

"E-health care is one of the few things in the last 50 years that could improve not only the quality of health care but its efficiency," said Laura D'Andrea Tyson, dean of UC Berkeley's Haas School of Business. >>



Amend C

Andrew Hassell

From: "Robert H. Shelton" <RbtShelton@worldnet.att.net>
To: "Andrew M Hassell" <ahassell@prodigy.net>; "John Sigalos" <jlsig1@airmail.net>
Sent: Thursday, July 06, 2000 3:29 PM
Subject: Privacy Technology Still Missing the Mark

Timely article that appeared in today's trade publication for ePharmaceuticals....

<< 5. PRIVACY TECHNOLOGY STILL MISSING THE MARK

A recent effort to improve online privacy by customizing Web browsers still has loopholes, according to an article in the San Francisco Chronicle. P3P, an emerging technology being developed by the World Wide Web Consortium, allows Internet users to specify what type of information a website can collect from them. Both Microsoft and Netscape are planning to install P3P technology in their next browser upgrades. The downside, according to the Chronicle, is that many sites may not choose to implement P3P. In addition, the software still doesn't control how websites use information that is collected with the users' permission.

http://www.epharm5.com/news.asp?an=SFC0018500452 >>

Here's what the summary referred to...

<< P3P Needs To Be Better At Privacy

Henry Norr
The San Francisco Chronicle

From Bill Clinton to Bill Gates, the establishment is rallying around a new Internet standard called P3P. It's an interesting development, but watch out for the hype they're spinning about it.

Although P3P (which stands for Platform for Privacy Preferences) is still just a working draft -- even after more than three years of development -- the White House, AOL, AT&T, Hewlett-Packard, IBM and even Procter & Gamble have already implemented it on their Web sites. Microsoft and Netscape plan to build support for it into the next release of their respective browsers.

According to the World Wide Web Consortium, the nonprofit but industry-dominated body sponsoring the standard's development, its purpose is to provide "a simple, automated way for users to gain more control over the use of personal information on Web sites they visit."

To judge by the spec and accompanying documentation at the P3P home page (www.w3.org/P3P), it will probably live up to that claim -- in a way. Its purpose is to define a standard, machine-readable language for describing privacy policies -- what kind of personal information a Web site proposes to collect from users and how it intends to use the data.

This turns out to require a surprisingly complex vocabulary. In addition to terms for many kinds of demographic information -- birth date, gender, home address and so on -- it also covers several types of dynamic data, such as the "referrer" (the site the user came from), the "clickstream" (exactly what the user clicks on while visiting a site) and what he or she may have searched for.

That's the easy part, though. The real challenge was to reduce the variety of ways a site might use such information to a handful of variables -- for example, how long the site will retain the information it collects, whether it will use the data to contact the individual to promote a product or service, whether it will compile data into profiles of user habits, whether such profiles will be anonymous or linked to personal identifying information, etc.

On the user side, a P3P-enabled browser would store the user's preferences about such matters, then compare those preferences to the policies of sites he or she visits. When the user -- call her Sally Surfer -- goes to a site whose policies match her preferences, she could cruise through it just as she does today, except that her browser might display an icon indicating that everything is hunky-dory from a privacy perspective.

Exactly what happens when Sally hits a site whose policies don't correspond to her preferences isn't defined in the current P3P spec; that's left up to the developer of the browser or other P3P- compliant software she's using.

Most likely, though, the program would put up a dialog box alerting Sally to the discrepancy and giving her a choice between accepting the site's policies or giving up her plan to visit it. Earlier drafts of the specification included a scheme for electronic haggling over such matters -- a way for users to get more benefits for providing more information -- as well as a mechanism for automatically transmitting personal data authorized by the user's preferences.

Those provisions, however, have been dropped -- the first because of its technical complexity, the second reportedly because polling showed widespread user resistance to background transfer of their personal information.

What's left is pretty modest, considering how long the standard has been in gestation and how many powerful players have been involved. As far as it goes, it strikes me as a modest step in the right direction.

But it's also a far cry from what we so obviously need: clear and enforceable rules about the collection and use of personal information. Consider:

-- Web site operators won't be under any obligation to implement P3P. Lots of them -- the sleazy, the lazy, those who lack the technical skills or software required -- will undoubtedly just ignore it. And it certainly doesn't address the problem of the failed dot- coms, which, as Cnet reported last week, are cheerfully auctioning off information about their former customers, possibly including phone and credit-card numbers, home addresses and purchase histories (news.cnet.com/news/0-1007-200-2176430.html?tag=st.ne.1002.tgif.ni)

-- Even if they're machine-readable, privacy policies are inevitably complex, so I suspect most users won't bother to configure the software for their own considered preferences -- they'll just accept the default settings.

-- Nothing in the standard says what those defaults should be. Because no user wants to be turned away from a site she's already navigated to, and most will find it burdensome and confusing to have to reconfigure their preferences before they can get where they're going, browsermakers will be under pressure from users as well as site operators to keep the bar low. (Don't forget: These are the same browsermakers who brought us the cookie -- and have since provided only the crudest tools for controlling this frightful mechanism.)

-- Neither technical standard can guarantee that sites actually do what they say they will, whether they state their policies in bits and bytes or in B2C bureaucratese. Nor can a standard impose any penalty on those who violate their commitments.

-- By accepting and formalizing the idea of trading personal data for access, P3P could have the effect of encouraging sites that don't collect such data to start doing so.

Despite all these shortcomings, many proponents of P3P are using it to justify their opposition to more meaningful solutions to the Internet privacy, such as laws of the sort that just about every other developed country already has -- and that we in the United States have enacted to protect other kinds of personal information, including telephone and video-rental records.

It's no wonder, then, that many seasoned privacy advocates are leery of P3P. The Electronic Privacy Information Center, a Washington, D.C., public-interest group that's been working on the issue for six years, and Junkbusters, an organization run by a computer scientist with a doctorate in data mining, have just issued a scathing critique under the title "Pretty Poor Privacy"

(www.epic.org/reports/prettypoorprivacy.html).

And even groups that support P3P acknowledge its limitations -- see, for example, the assessment produced by the Center for Democracy and Technology in cooperation with the office of Ontario's Information and Privacy Commissioner, which is posted at www.cdt.org/privacy/pet/p3pprivacy.shtml.
Something here.

NIXON TO THE RESCUE? One irony about the sad state of privacy protection in the United States: This country isn't just the home of the Bill of Rights and what Justice Louis Brandeis called "the right to be let alone" -- it's also the home of the principles on which Europe's computer-era privacy regulations are based. Known as the Code of Fair Information Practices, these guidelines were developed by a commission set up by, would you believe, the Nixon administration. (I owe that tidbit to "Database Nation," Simson Garfinkel's excellent new book on the privacy problem, published by O'Reilly.)

Here are the five key principles of the code, as articulated (according to Garfinkel) in a 1973 report of the then Department of Health, Education and Welfare:

-- There must be no personal data record-keeping system whose very existence is secret.

-- There must be a way for a person to find out what information about the person is in a record and how it is used.

-- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

-- There must be a way for a person to correct or amend a record of identifiable information about the person.

-- Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Giving these principles the force of law is no privacy panacea -- there isn't one -- but at least it would get at the heart of the problem, which is more than one can say about P3P. >>